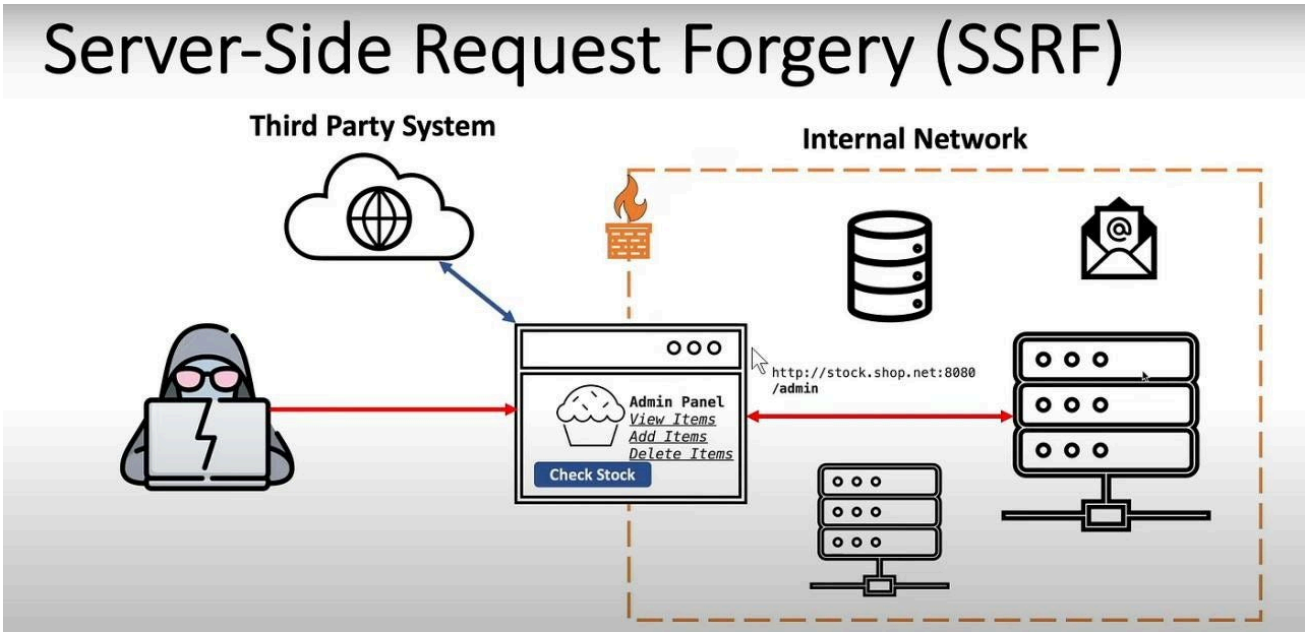
SSRF Explain (Server-Side Request Forgery)

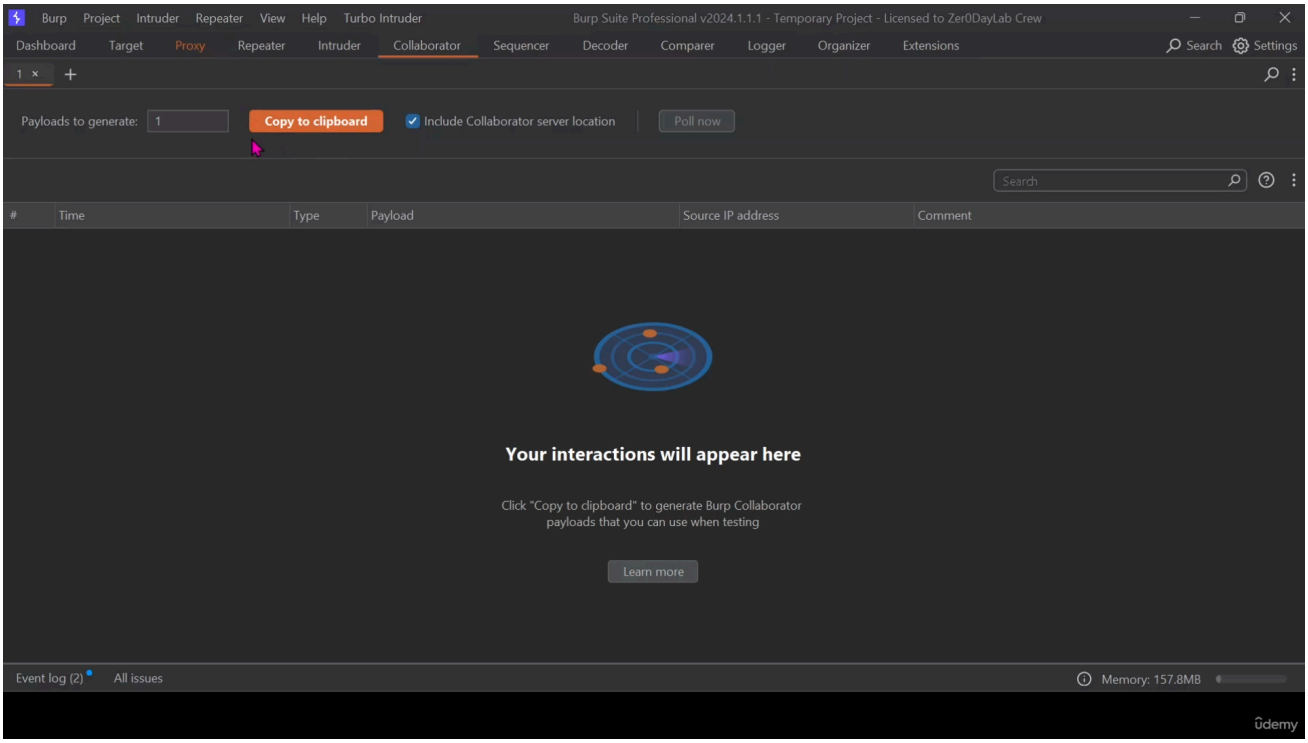
- الثغرات بتتقسم لنوعين :
- الـ server side : ثغره بتقدر توصل للـ server زي (SQL injection . SSRF)
- الـ client side : ثغره بتاثر فالعميل نفسه مش بتاثر ف ال server زي (XSS.CSRF)

- 

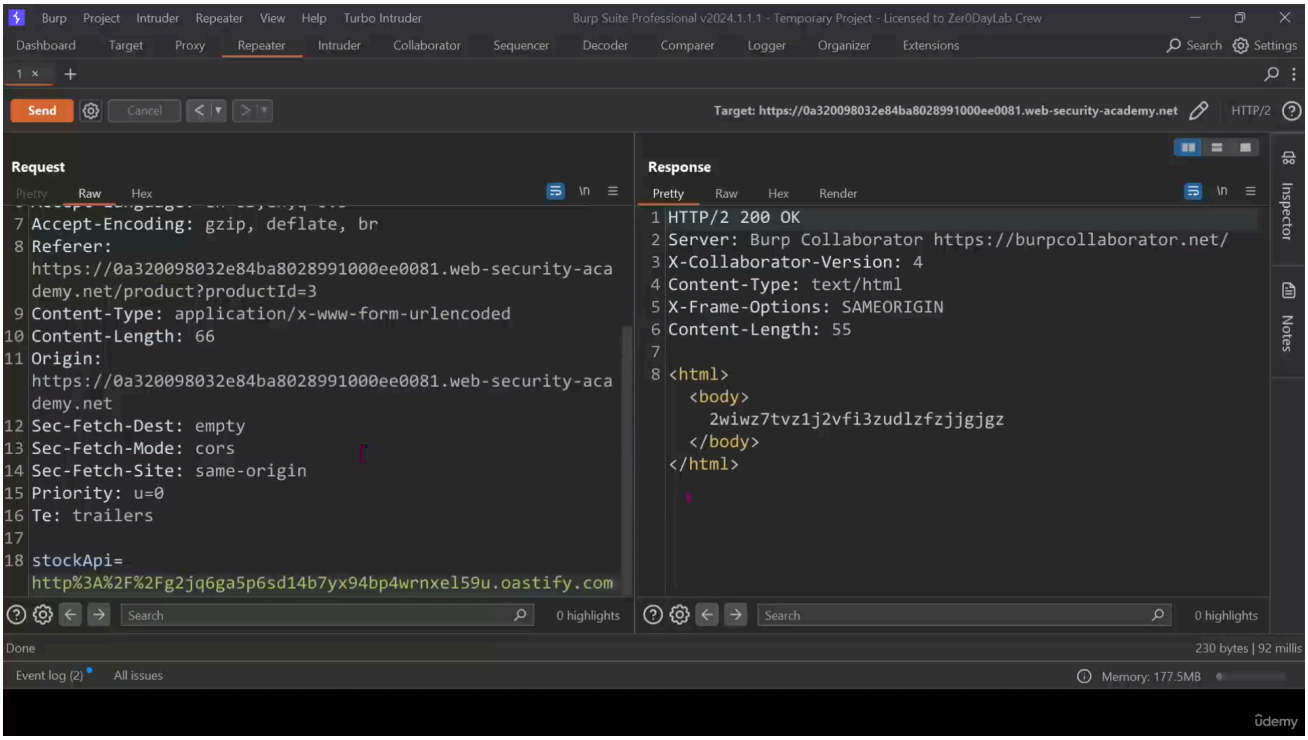
- في حاجات زي الصور وفالديوهات بيبقي الموقع مستضيها من سيرفر تاني مثلا
- انت لما بتعوزها او تيجي تفتحها الموقع بيطلبها من السيرفر فانت بتوقف الطلب

- ```
  Pretty Raw Hex
  1 POST /product/stock HTTP/1.1
  2 Host: 0a320098032e84ba8028991000ee0081.web-security-academy.net
  3 Cookie: session=vzYjb4pMEVt1CIAVVTEHPEwLCq9Io0d9
  4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
  5 Accept: */*
  6 Accept-Language: en-US,en;q=0.5
  7 Accept-Encoding: gzip, deflate, br
  8 Referer: https://0a320098032e84ba8028991000ee0081.web-security-academy.net/product?productId=3
  9 Content-Type: application/x-www-form-urlencoded
  0 Content-Length: 107
  1 Origin: https://0a320098032e84ba8028991000ee0081.web-security-academy.net
  2 Sec-Fetch-Dest: empty
  3 Sec-Fetch-Mode: cors
  4 Sec-Fetch-Site: same-origin
  5 Priority: u=0
  6 Te: trailers
  7 Connection: close
  8
  9 stockApi=http%3A%2F%2Fstock.weliketoshop.net%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D3%26storeId%3D1
  ```

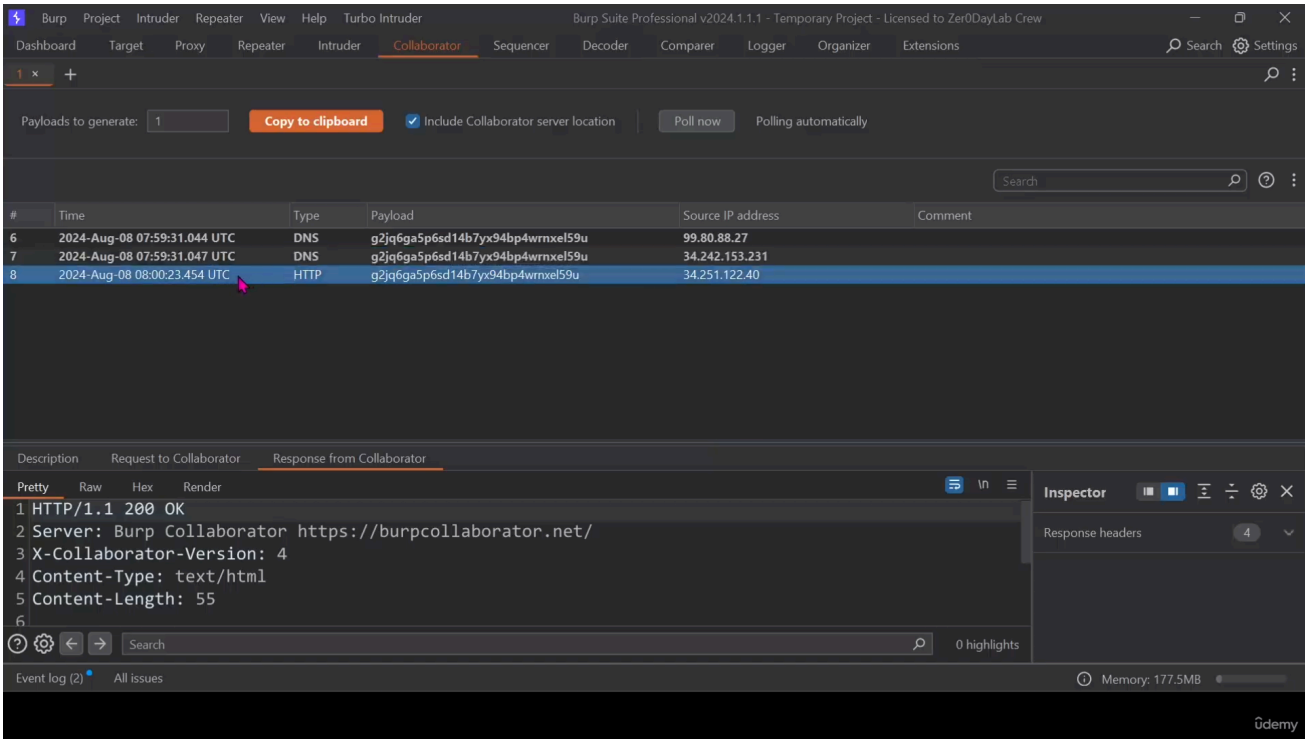
- دا بيبقي شكل الطلب بيبقي زي كدا انت بتشيل كل رابط وتجرب مكانو رابط الموقع المصاب بتاعك
- لو معندكش ممكن تستخدم ال collaborator من burp بس النسخه البرو بس
  ```



- بتشغله وتضغط علي copy to clipboard بتبقي نسخت الرابط وتجرب تحطو بدل الرابط وتشوف الناتج

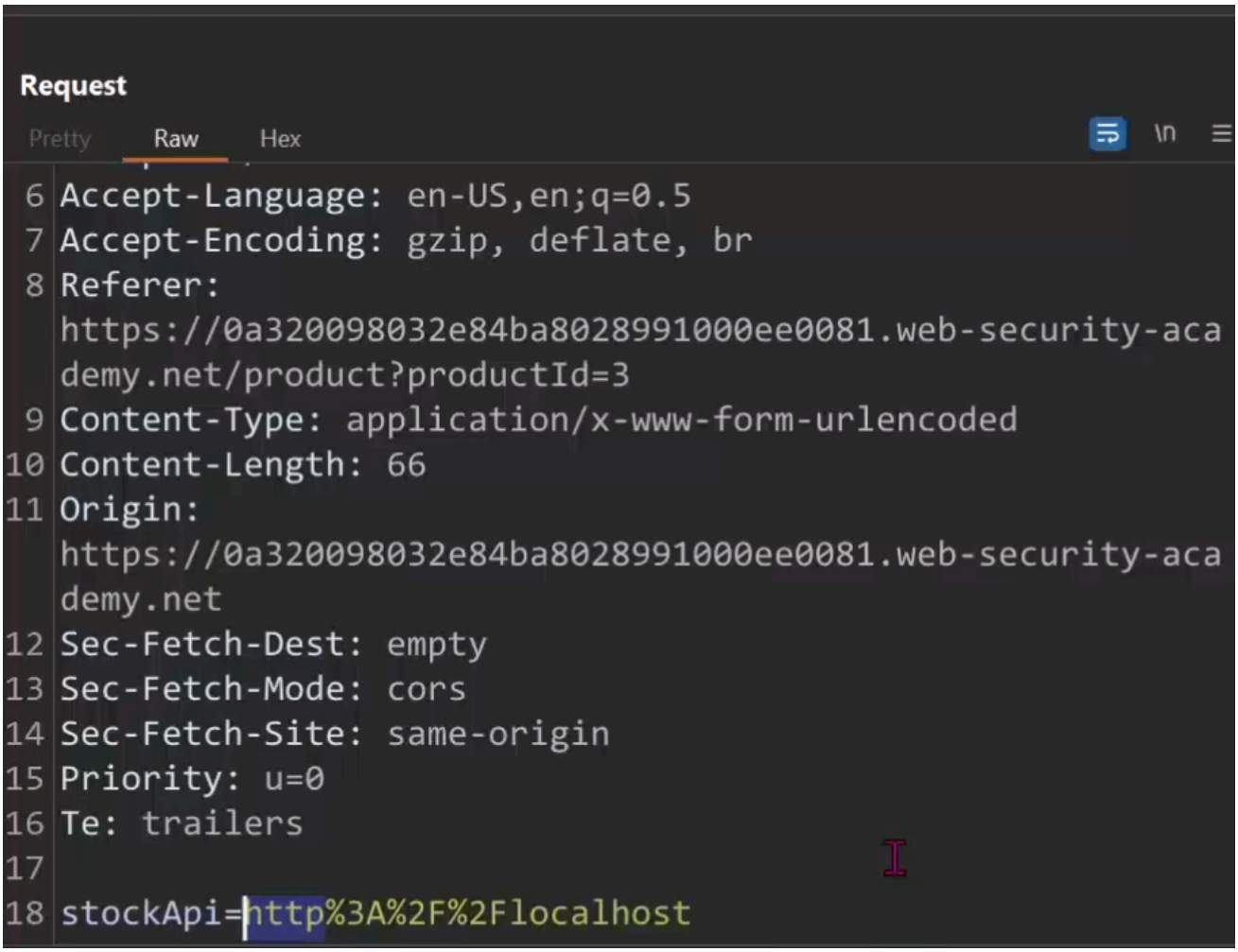


- لو اداك 200 ok كدا تمم
- علشان تشوف الرد بتروح علي collaborator وبتضغط علي poll now هيظهرلك النتايج

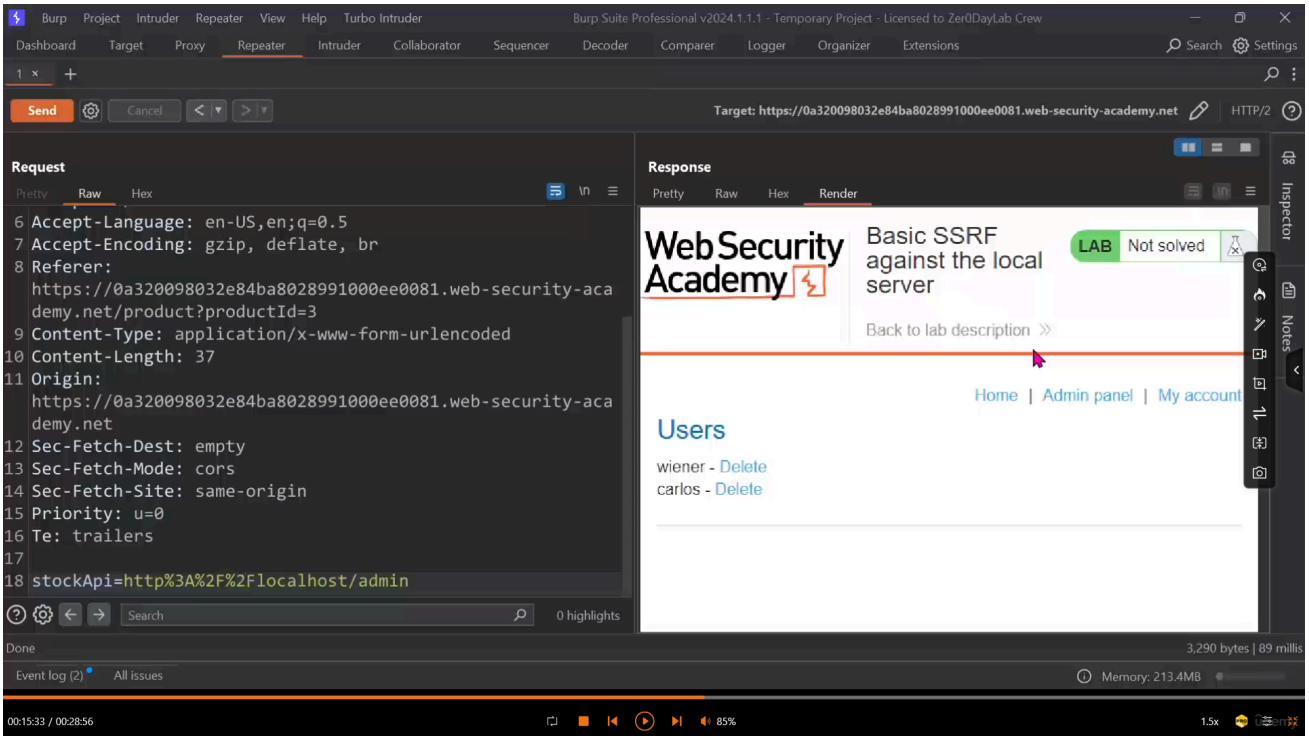


- لو ظهرلك http كدا يعتبر ثغره وممكن تبلغها لكن لو Dns بس مش ثغره

- استغلال الثغره

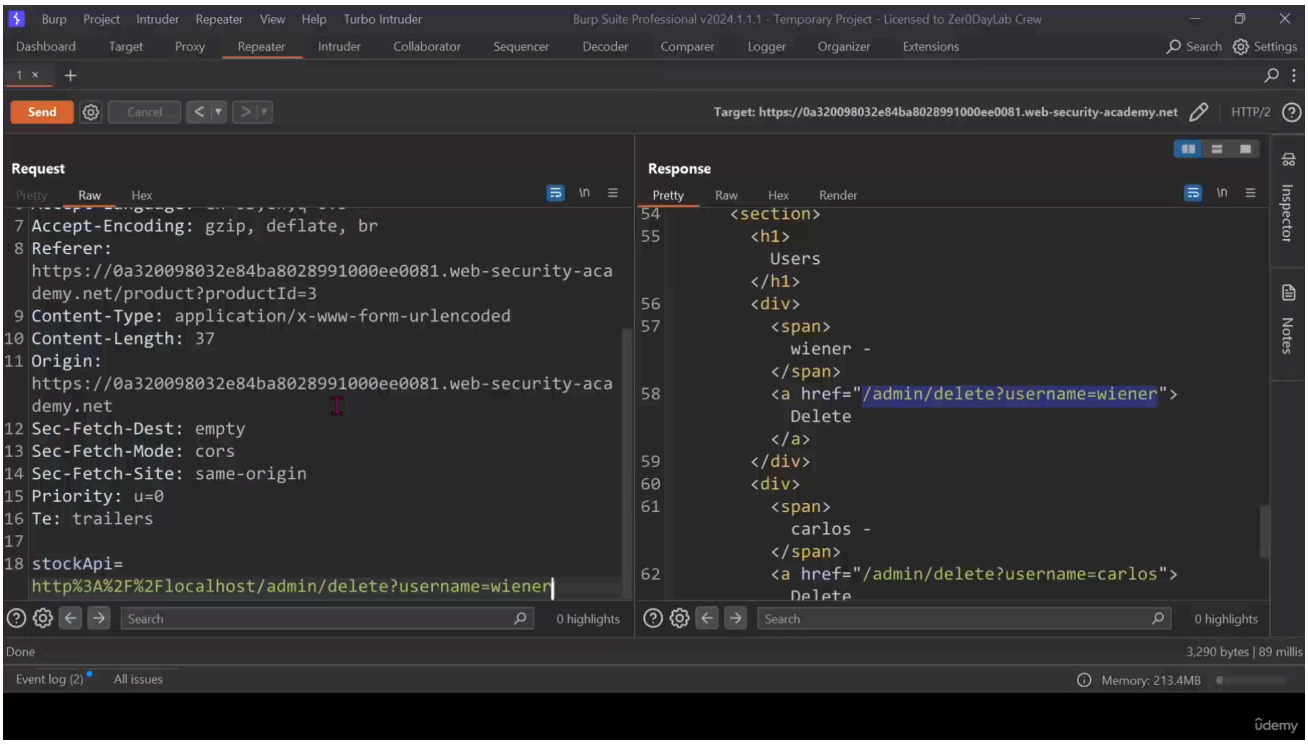


- ممكن تشيل رابط ال collaborator وتحط مكانو localhost

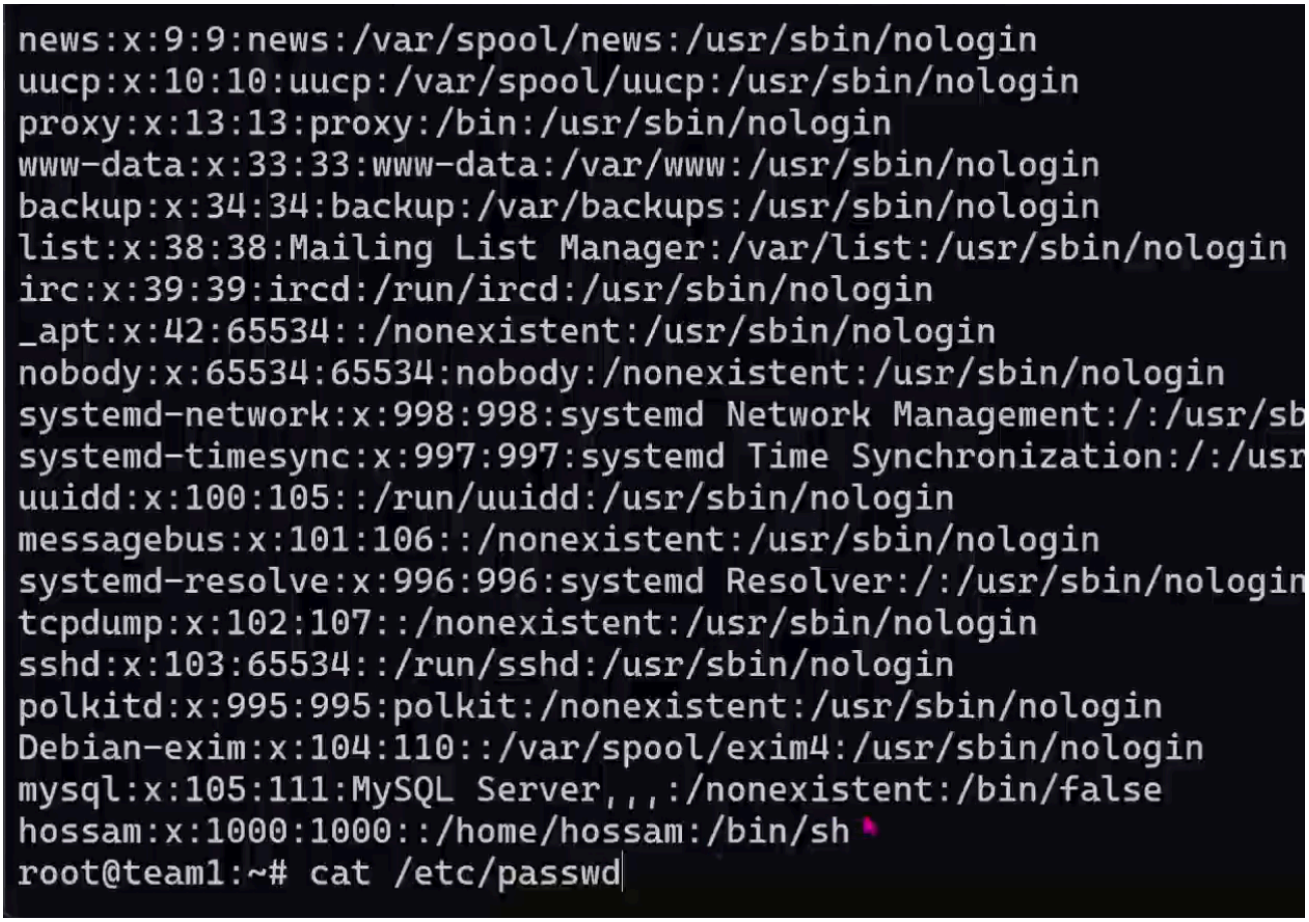


- وممكن لو زودت ادمن يضيفك مميزات اكتر

- ممكن بقي تقدر تمسح ال user او تعمل اي حاجه ك ادمن



- بتجرب مكان كل رابط بتحط رابط الـ collaborator



- الملف /etc/passwd الملف دا بيثبت انك استغليت الثغره

- ممكن تستخدم tool ف الـ burp اسمها collaborator Everywhere دي بتعمل مكانك كل حاجه بتغير الروابط برابط ال collaborator والناتج بيظهر هنا